Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report for 10 September 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- In a report released Wednesday, the Federal Energy Regulatory Commission said that utilities vary widely in how they manage vegetation surrounding their high−voltage electric transmission lines. (See item 2)
- The Associated Press reports interference from cell phones on the 800−megahertz band of the radio−frequency spectrum is an ongoing problem confronting firefighters, police, and emergency medical workers across the country. (See item 22)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *September 10, Gloucester County Times (NJ)* — **Gasoline reported missing. Over 70,000 gallons of gasoline have been reported missing from a gas station according to Washington Township, NJ, police reports.** In June, the owners of US Gas were told to close by the New Jersey Department Environmental Protection because the underground tanks at the station had expired and needed to be changed. On September 3, a US Gas employee, told police that a company hired to siphon remaining gas from the underground tanks had found nothing to remove. Missing from the tanks were gasoline and diesel fuel valued at $20,047. When the state ordered the closing of the gas station, the electricity at the station was also shut down. No surveillance system was used at the station, police reports state.
Source: http://www.nj.com/news/gloucester/local/index.ssf?/base/news

−7/1094717701191040.xml

2. *September 09, Washington Post* — **Utilities uneven in managing vegetation. In a report released Wednesday, September 8, the Federal Energy Regulatory Commission (FERC) said that utilities vary widely in how they manage vegetation surrounding their high−voltage electric transmission lines.** The report includes a number of recommendations for making the electricity grid more reliable −− including mandatory standards for trimming trees. The report was prompted by the blackout of August 14, 2003, which was in part caused by FirstEnergy Corp.'s failure to adequately prune trees near its electrical lines. In April 2004, the FERC ordered those who own, control or operate the highest−voltage portions of the nation's electrical grid to provide information on their vegetation management practices. **The report concluded that transmission owners and operators have performed extensive vegetation management, and while this does not guarantee grid reliability, the reduced vegetation represents a positive reduction of risk of interference along the nation's high−voltage transmission network.** Many utilities reported to the FERC that their efforts to keep vegetation away from transmission lines were impeded by federal and state regulations. Some said that state governments had hindered their efforts to improve electrical reliability.
Report: http://www.ferc.gov/industries/electric/indus−act/reliabilit y/veg−mgmt−rpt−final.pdf
Source: http://www.washingtonpost.com/wp−dyn/articles/A6663−2004Sep8 .html

3. *September 09, Mercury News (CA)* — **Heat brings record energy use. California power demand peaked at 45,597 megawatts Wednesday, September 8, topping Tuesday's record of 45,165 megawatts, according to the California Independent System Operator, which runs the high−voltage grid.** A megawatt is enough to power about 750 homes. Wednesday marked the seventh time this year power use set a record. The recent heat wave is only unusual for how long it has loomed, says National Weather Service forecaster Steven Anderson. Grid managers expect power demand to fall Thursday to a peak of 44,127 megawatts but urge consumers to avoid electricity use from 4:00 to 7:00 p.m., when demand peaks. Until this year, the state's record for power use was 43,609 megawatts, set in July 1999.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/states /california/peninsula/9616546.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *September 08, Associated Press* — **Chemical spill in Wilmington.** Hazmat teams rushed to the scene of a chemical spill at a pharmaceutical manufacturing plant near downtown Wilmington, DE, on Wednesday, September 8. Authorities say the spill was reported at Noramco of Delaware around 4 p.m. after a vessel being filled with the petroleum solvent toluene overflowed. **Officials say 300 to 500 gallons of the highly volatile chemical spilled. Most of it flowed into the plant storm drainage system and on into the Christina River.** Emergency responders put a boom around the drainage pipe to prevent further discharge. But authorities say there was little they could do about the toluene that had already reached the river. David Small of the Department of Natural Resources and Environmental Control says the chemical is difficult to capture.
Source: http://kyw.com/Local%20News/local_story_252220343.html

[Return to top]

Defense Industrial Base Sector

5. *September 09, Reuters* — **Plant suspends bunker buster bomb production. The factory that manufactures nearly all the bombs for the U.S. military has suspended production of "bunker buster" penetration bombs after workers at the plant developed anemia,** officials said on Wednesday, September 8. The 2,000−pound "bunker buster" bombs are designed to penetrate the surface and do damage to structures below. Production was halted in August at the McAlester Army Ammunition Plant (MCAAP), in eastern Oklahoma, after workers making that type of munition tested positive for the blood disease anemia, plant officials said. Their anemia was likely caused by exposure to the explosive TNT. A heavy production schedule may also have resulted in higher TNT exposure for workers. Production will be halted until at least January 1. Production of other types of bombs will continue at the plant. Built in 1943, the **McAlester plant employs about 1,400 workers who produce the overwhelming majority of the bombs used by the United States military,** including most of the bombs dropped since the beginning of the wars in both Afghanistan and Iraq.
Source: http://www.reuters.com/newsArticle.jhtml?type=domesticNews&s toryID=6187187

[Return to top]

Banking and Finance Sector

6. *September 09, Department of Treasury* — **U.S. designates foundation as linked to terror. The Department of Treasury announced on Thursday, September 9, the designation of the U.S. branch of the Saudi Arabia−based Al Haramain Islamic Foundation (AHF), along with one of its directors, Suliman Al−Buthe. In addition, the AHF branch located in the Union of the Comoros was also designated Thursday.** The assets of the U.S. AHF branch, which is headquartered in Oregon, were blocked pending investigation on February 19, 2004. The investigation shows direct links between the U.S. branch and Osama bin Laden. Additionally, the affidavit alleges the U.S. branch of AHF criminally violated tax laws and engaged in other money laundering offenses. Information shows that individuals associated with the branch tried to conceal the movement of funds intended for Chechnya by omitting them from tax returns and mischaracterizing their use, which they claimed was for the purchase of a prayer house in Springfield, MO. Other information available to the U.S. shows that funds that were donated to AHF with the intention of supporting Chechen refugees were diverted to support mujahideen, as well as Chechen leaders affiliated with the al Qaeda network.
Source: http://www.treasury.gov/press/releases/js1895.htm

7. *September 08, ComputerWorld* — **For Wall Street, 9/11 lessons three years in the making.** With the third anniversary of the September 11, 2001, terrorist attacks approaching this weekend, senior Wall Street executives on Wednesday, September 8, outlined for Congress unprecedented security measures that continue to be revised and improved to withstand what the government fears is an ongoing effort by al Qaeda to disrupt the U.S. economy. **Appearing at a House Financial Services committee hearing, senior government officials and**

executives from key financial institutions described in startling detail the efforts that continue to go into bolstering physical and cyber security for the nation's critical financial trading systems. However, despite these efforts to bolster physical security and network redundancy, Wayne A. Abernathy, assistant Treasury secretary for financial institutions, warned Congress that the financial sector is under constant electronic assault by both organized crime and unknown entities. "These assaults have progressed from computer hackers and pranksters into theft and now, we believe, on to schemes to disrupt the operations of our financial systems," he said. "Some of these attacks have their sources in organized crime [and] we believe that, increasingly, still more sinister actors are involved. The threat is not theoretical."
Source: http://www.computerworld.com/printthis/2004/0,4814,95765,00. html

8. *September 07, Mainichi Daily News (Japan)* — **Customers' info leaked from major credit card firm.** Personal information on as many as 571 customers of major Japanese credit card firm UC has been leaked, with information on 88 cardholders used to make illicit purchases totaling over US$122,000, the firm has announced. UC officials said the purchases included transactions made over the Internet. UC will pay for the damages and issue new cards to all 571 people involved. Beginning in January this year, repeated fraud involving purchases made over the Internet occurred. Police arrested one suspect who made an illicit purchase in April. **Subsequent investigations revealed that a former employee carrying out work on commission for the card firm used a computer terminal to obtain customers' information then sold it.** UC confirmed that between November last year and April this year, the former employee had handled information on 571 customers, and that there was a possibility this information had been leaked.
Source: http://mdn.mainichi.co.jp/news/20040907p2a00m0dm001000c.html

[Return to top]

Transportation Sector

9. *September 09, Government Accountability Office* — **GAO−04−1001: Border Security: State Department Rollout of Biometric Visas on Schedule, but Guidance Is Lagging (Report).** As a complement to the Department of Homeland Security's (DHS) United States Visitor and Immigrant Status Indicator Technology (US−VISIT) program—a government−wide program to better control and monitor the entry, visa status, and exit of visitors—the State Department (State) is implementing the Biometric Visa Program at all 207 overseas consulates by October 26, 2004. This program, required by the Enhanced Border Security and Visa Entry Reform Act of 2002, requires that all persons applying for U.S. visas have certain biometrics (fingerprints) and a digital photograph collected during the visa application interview. This information must be cleared through the DHS Automated Biometric Identification System (IDENT) before an applicant can receive a visa. GAO reviewed State's rollout of the program, including its implementation progress and how State and DHS envision the program being used to help adjudicate visas. **The Government Accountability Office (GAO) recommends that DHS and State develop and provide to consular posts guidance on how the program should be used to help adjudicate visas and that State direct each consular post to develop an implementation plan based on this guidance.** DHS and State generally concurred with these recommendations. Highlights: http://www.gao.gov/highlights/d041001high.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?

10. *September 09, Government Accountability Office* — **GAO−04−1080T: Border Security: Joint, Coordinated Actions by State and DHS Needed to Guide Biometric Visas and Related Programs (Testimony).** Since September 11, 2001, the U.S. government has made a concerted effort to strengthen border security by enhancing visa issuance policies and procedures, as well as expanding screening of the millions of foreign visitors who enter the United States annually. Consistent with the 9/11 Commission report that recommends a biometric entry−exit screening system for travelers, the Department of State's biometric program complements the Department of Homeland Security's (DHS) United States Visitor and Immigrant Status Indicator Technology (US−VISIT) program—a government−wide program to better control and monitor the entry, visa status, and exit of visitors. GAO was asked to present the findings of its report on State's Biometric Visa Program, as well as discuss other aspects of visa processing and border security that require coordinated, joint actions by State and DHS. **The Government Accountability Office (GAO) has recommended that DHS and State develop and provide guidance to consular posts on how to use information from the biometric program to adjudicate visas.** In other reports, GAO has made recommendations to DHS and State to improve US−VISIT, as well as several aspects of the nonimmigrant visa process. The agencies generally agreed and are taking actions to implement our recommendations. Highlights: http://www.gao.gov/highlights/d041080thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−1080T

11. *September 09, Insight* — **U.S. ports unsecured.** A study says port facilities in New York and New Jersey need a cyber backbone and more planning to improve security against a terrorist attack. Researchers at the Stevens Institute in Hoboken, NJ, found the ports lacked well−coordinated, integrated plans to prevent and respond to attacks. Officials also needed to establish an electronic or cyber backbone for secure, redundant communications and an effective means of responding to multiple events. **The report suggested network−centric operations as the way to improve security. This approach, developed by the U.S. military, relies on communications and computers to inform all the individuals involved of what is going on so they can better coordinate their actions.** "When the FBI named the stretch of land between Port Newark and Newark Liberty Airport as the two most dangerous miles in America, the urgency to improve port security in the New York and New Jersey region became undeniably clear," says Jerry MacArthur Hultin, dean of the Howe School of Technology Management at Stevens Institute of Technology, and formerly under secretary of the Navy.
Source: http://www.insightmag.com/news/2004/09/06/National/U.Ports.Unsecure.Still−714041.shtml

[Return to top]

Postal and Shipping Sector

12. *September 09, Government Accountability Office* — **GAO−04−239: U.S. Postal Service: Better Guidance Is Needed to Ensure an Appropriate Response to Anthrax Contamination (Report).** In September and October 2001, at least four letters containing anthrax spores were mailed to news media personnel and two U.S. Senators. Nine postal employees associated with two postal facilities that processed the letters −− Trenton in New

Jersey and Brentwood in Washington, DC −− contracted anthrax and two Brentwood employees died. The U.S. Postal Service closed Trenton and Brentwood, but other contaminated postal facilities remained open. **According to Postal Service managers, public health officials, and union representatives, the Postal Service considered the health risks to its employees ahead of its mission to deliver the mail in deciding whether to close postal facilities.** The Postal Service relied on public health agencies to assess the health risks to its employees. These agencies believed the risks to be minimal until the Centers for Disease Control and Prevention (CDC) confirmed cases of anthrax in postal employees at Trenton and Brentwood. The Postal Service then closed these facilities. **Public health agencies underestimated the health risks to postal employees, in part, because they did not know that anthrax spores could leak from taped, unopened letters in sufficient quantities to cause a fatal form of anthrax.** The Postal Service kept the three other facilities covered by General Accountabilty Office's review open because public health officials had advised the agency that employees at those centers were at minimal risk.
Source: http://www.gao.gov/new.items/d04239.pdf

[Return to top]

Agriculture Sector

13. *September 09, U.S. Newswire* — **Kansas State University's National Agricultural Biosecurity Center. The Department of Defense has awarded a $1.38 million two−year contract to the National Agricultural Biosecurity Center at Kansas State University. Through efforts by the National Agricultural Biosecurity Center and its three subcontractors, the project will develop content and software to help the nation's emergency management personnel respond more effectively to an agricultural or zoonotic bioterrorist event.** The project is called "Situational Competency, Simulations and Lessons Learned for Food/Agricultural Bioterrorism." As partners on the project, Analytic Services, Inc., will compile an agrosecurity lessons learned database based on modifications of existing software; Cell Exchange will create a "dashboard technology" based on its "Protect America" real time content aggregation system; and the University of Alabama−Birmingham will create a series of rotating images to increase awareness of agricultural biopreparedness. Plans are to create an integrated system accessible to the end−users via the Internet.
Source: http://releases.usnewswire.com/GetRelease.asp?id=35878

14. *September 08, Agriculture Online* — **Two states offer online tools to register animal premises.** Several state departments of agriculture have begun the task of identifying the farms, feedlots, sales barns, and slaughter facilities that handle food animals within their state's borders. This is the first step toward the implementation of a national animal identification system that will enable livestock and poultry to be rapidly traced from the farm to the dinner fork. Illinois and Wisconsin are part of a five−state consortium that will develop and implement the national animal identification system in the Great Lakes region. **Illinois' Agriculture Department has established an online registration process to identify food animal facilities. The goal in Illinois is to identify every food animal facility by September 1, 2005.** Menus are provided to ease the process and ensure similar facilities are categorized the same way. After the form is submitted, the facility will be issued a federal premise identification number. **In Wisconsin, any facility or operation that handles livestock can register on a**

voluntary basis using the system that will be used when registration becomes mandatory on January 1, 2006.
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=goDetail__ANewsindex_html___52468___1

[Return to top]

Food Sector

15. *September 07, North Carolina State University* — **Researchers work to keep milk supply free of contaminants. The more than nine million cows that produce milk in the U.S. occasionally need to be treated for various ailments, so researchers at North Carolina State University's College of Veterinary Medicine are working to protect that commodity by helping to keep contaminants out of the milk supply.** Geof Smith, assistant professor of ruminant medicine, is studying how long the residue of pharmaceuticals remains in cow's milk. When a dairy cow is given antibiotics or other drugs, the milk that cow produces must be discarded until the drugs clear the cow's mammary system. Smith's work is part of the Food Animal Residue Avoidance Data Bank (FARAD), a support system designed to provide livestock producers and veterinarians with information on how to avoid drug, pesticide, and environmental contaminant residue problems. The antibiotic Ceftiofur is used to treat a number of problems in cows. Ceftiofur is approved for injection into the muscle and under the skin, but, according to Smith, some farmers have injected Ceftiofur directly into the mammary glands. Smith's research involved using the drug in five dairy cows. He took milk samples at milking time twice a day, for 10 days. He then used chromatography analysis to measure the drug's concentration in the milk and determine how long it remained present.
Source: http://www.ncsu.edu/news/press_releases/04_09/240.htm

[Return to top]

Water Sector

16. *September 09, Virginian−Pilot* — **Waves of dead fish washing ashore. Thousands of dead croakers have washed ashore on Virgina beaches in recent days. Some scientists believe a bacterium is responsible for mortalities from Delaware to southeast Virginia – and now in Florida, too. The researchers, though, have not been able to isolate or define any suspected aquatic bug, or explain why only Atlantic croakers have been struck.** Other theories include cold−water jolts, or upwelling, that shock weakened croakers as they swim along the mid−Atlantic coast, or a mysterious virus of some sort. A team of scientists from Virginia, Maryland, Delaware, and Florida is continuing to dig for answers. The croakers are apparently suffocating, their gills left bleeding. In some cases, they have been seen swimming incoherently near the water's surface −− odd behavior for a bottom−feeding fish. "No one has indicated that they have ever seen anything like this," where only adults of one fish species are dying over such a large geographic area, said Roger Everton, a water−quality expert with the Virginia Department of Environmental Quality.
Source: http://home.hamptonroads.com/stories/story.cfm?story=75345&r an=100461

17. *September 09, Journal−Pioneer (Canada)* — **Pesticide found in water sample. A trace amount of a pesticide has been found in one water sample taken from the Middleton, Canada, site of a fish kill reported last week.** But it's difficult to say what role the chemical had in the death of trout in Middleton or Wright's Pond, says Bruce Birch, an enforcement officer with Environment Canada. Staff with the Province collected about 400 dead fish, almost all brook trout. **In an interview, Birch said according to an Environment Canada lab a trace amount of the fungicide chlorothalonil had been found in one water sample.** Birch said three water samples had been checked for pesticides. He said the other water samples didn't show any detectible amounts. **And he added a trace amount means it's still below toxic levels.** "It means it's there but very, very low." He said that means it's "really difficult" to say whether it's unlikely or likely it lead to the death of the fish. Birch said there are still results of tests on fish and sediment come back. But he said the fish were pretty decomposed when picked up. That means the chances of finding the cause of death are pretty remote.
Source: http://www.journalpioneer.com/news.aspx?storyID=21036

18. *September 09, Associated Press* — **Hurricane leaves water shortage in Asheville. Tens of thousands of households in Asheville, NC, and at least five other mountain towns remained without drinking water Thursday, September 9, due to washed−out water lines or sanitation systems flooded by the remnants of Hurricane Frances.** The storm, downgraded to a tropical depression, drenched western North Carolina and the state's Sandhills region Tuesday and Wednesday, dropping more than a foot of rain on some mountain communities. Twelve western counties declared a local state of emergency, and Governor Mike Easley declared a statewide emergency. The Regional Water Authority of Asheville, Buncombe and Henderson counties lost all water transmission lines from the North Fork Water Treatment Facility because of flooding.
Source: http://www.wilmingtonstar.com/apps/pbcs.dll/article?AID=/20040909/APN/409090596&cachetime=5

19. *September 08, DOE/Sandia National Laboratories* — **Sandia water experiments. A method that uses roughly only one−hundredth the fresh water customarily needed to grow forage for livestock may leave much more water available for human consumption, as well as for residential and industrial uses.** The method for lessening water use is being tested by 42 wireless sensors being installed in a forage−growing hydroponic greenhouse under the supervision of the National Nuclear Security Administration's Sandia National Laboratories, a U.S. national security lab. **"A large proportion of freshwater usage around the world is agricultural. The ability to reduce the amount of water needed for it and thus lessen the possibility of international conflict is extremely important to the security of the U.S. and the world,"** said Sandia's director for Geoscience and Environment Peter Davies. Preliminary indications are that hydroponic greenhouses in New Mexico, for example, could reduce the current 800,000 acre−feet of water to 11,000 acre−feet to produce an equivalent amount of livestock forage, and do this on less than 1,000 acres instead of 260,000 acres −− the current amount used for New Mexico production of alfalfa. Similar conditions of water use exist in many places in the world.
Source: http://www.sandia.gov/news−center/news−releases/2004/gen−science/greenhouse.html

[Return to top]

Public Health Sector

20. *September 09, Houston Chronicle (TX)* — **Doctors examine death of seafarer. Pathologists donned protective suits and germ−fighting respirators Wednesday, September 8, as they conducted an autopsy on the body of a seafarer who may have died from the common West African disease called Lassa fever.** The man's body was brought from the quarantined cargo ship Overseas Marilyn to the Galveston, TX, medical examiner's office Sunday, September 5. Investigators described the man, an American whose name was not released, as healthy and in his 30s. Although Lassa fever is hard to contract, Galveston County Chief Medical Examiner Stephen Pustilnik closed down the building in which his facilities are located during the autopsy to avoid the risk of anyone becoming infected with any disease the victim might have contracted. The man first showed symptoms on August 25 and died on August 31. On that day, the ship's operators, Connecticut−based OSG Shipping Management Inc., contacted Galveston County health officials for advice on how to guard against any infection spreading among the crew or on shore. **It was decided the ship with 19 people on board will remain offshore near Galveston under voluntary quarantine until pathologists and U.S. Centers for Disease Control and Prevention scientists determine the cause of the man's death.**
    Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/278556 8

21. *September 08, Pharmacist* — **Counterfeit medications pose international challenge. Pharmacists need to talk to patients about the dangers and prevalence of counterfeit medications and report suspect products to authorities, according to a working group of the International Pharmaceutical Federation (FIP).** Jane Nicholson, of the United Kingdom, Lowell J. Anderson, of White Bear Lake, MN, noted that both developing and developed countries are encountering serious and widespread problems with counterfeit medications. While the pharmaceutical industry is working on sophisticated electronic bar coding and some governments have implemented sequential numbering and reconciliation processes for individual packages, Nicholson and Anderson explained that no single magic bullet will stop counterfeiters. A global alliance has been formed by the World Health Organization (WHO), FIP, the World Medical Association, UNICEF, and Interpol in an effort to combat counterfeiting.
    Source: http://www.pharmacist.com/articles/h_ts_0621.cfm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *September 09, Associated Press* — **Pennsylvania firefighters battle new threat to public safety.** In some of Philadelphia's most heavily populated neighborhoods −− Center City, Grays

Ferry and University City −− cell−phone signals have blocked radio communication for firefighters at the scene of fires, department officials confirm. **Interference from cell phones on the 800−megahertz (MHz) band of the radio−frequency spectrum is a problem confronting firefighters, police, and emergency medical workers across the country. Fire and police units in Philadelphia suburbs such as Upper Merion and East Norriton have complained of cell−phone interference. In New Jersey, state police have received reports of interruptions in every part of the state.** Last month, the Federal Communications Commission proposed moving all cell−phone carriers to one end of the 800−MHz band and all public−safety users to the other. But any agreement would need the approval of Nextel Communications Inc. of Reston, VA, the largest commercial user of frequencies in the 800−MHz range. The plan calls for Nextel to acquire a new band of spectrum worth $4.8 billion. In return, the company would have to pay to reconfigure public−safety signals in the 800−MHz range.
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=46&id=34950

23. *September 09, The Register (MA)* — **Training exercise will help prepare emergency responders.** The Cape Cod Medical Reserve Corps, in South Dennis, MA, was conceived and funded with the goal of becoming part of the emergency management system. "They began with a focus on Dennis, and have been there to relieve paramedics, assist at emergency shelters and work with the Red Cross," Dennis police Lt. Peter Benson said. **The group is striving for certification as an emergency medical shelter. A controlled test is planned Saturday, October 30 to measure how timely the response would be in the event of a crisis.** "It will be a mass flu vaccination clinic in which we will strive to vaccinate 2,500 people in eight hours to see if we could do it in an emergency. We've been planning this since last November," said Benson. The flu vaccine will be supplied by the Strategic National Stockpile, and those vaccinated will include first responders, teachers and their families in Dennis, Yarmouth and Barnstable. Volunteers for the test clinic include Dennis police, nurses, doctors and members of the medical reserve corps. Various private companies and agencies will provide transportation
Source: http://www2.townonline.com/barnstable/localRegional/view.bg? articleid=81924

24. *September 08, WCPO (OH)* — **Mock disaster drill reveals communications gap.** Butler County, PA, emergency workers found out how prepared they were for a disaster during the county's full−scale homeland security drill on Wednesday, September 8. It looked like a real disaster. Emergency workers from every Butler County community rushed to respond to the mock terror attack as dozens of people pretended to need medical attention. Area communications leaders say the drill helped them spot a serious problem in Butler County. **"Problem is, you've got different radio systems, different departments on different radios," said Frank Young, of Warren County, OH, Emergency Services, "and in order to communicate they're doing well, they have a joint command center, but out and about −− they aren't sure of precisely what's going on." Butler County emergency leaders say they've asked for a county−wide communication system before.** They're hoping the problems discovered from this week's disaster drill will push community leaders to support one.
Source: http://www.wcpo.com/news/2004/local/09/08/silverman.html

[Return to top]

Information Technology and Telecommunications Sector

25. *September 09, The Register (UK)* — **Telenor takes down 'massive' botnet.** A network of more than 10,000 zombie PCs has been dismantled after security staff at Norwegian telco Telenor located and shutdown its controlling server. These expanding networks (dubbed 'botnets' by the computer underground) can be used for spam distribution or as platforms for Distributed Denial of Service (DDoS) attacks. By using compromised machines − instead of open mail relays or unscrupulous hosts − spammers can bypass IP address blacklists. **The clients of the Telenot botnet remain compromised, even though the controlling server has been taken out. The Internet Storm Center advises users with network traffic logs to check for connections from their network to the IRC Server − which was listening on IP 203.81.40.172 tcp port 10009.** The Telenor takedown is a significant step in the fight against botnets, which have been implicated in recent DDoS attacks against Akamai and DoubleClick. **Last month, the FBI shut down a large IRC provider after uncovering evidence it was a middleman between hackers with access to botnet networks and businesses prepared to launch denial of service attacks on rivals.**
Source: http://www.theregister.co.uk/2004/09/09/telenor_botnet_disma ntled/

26. *September 09, USA Today* — **Tech industry presents less−than−unified defense. As cybercriminals toil with near impunity, tech companies in the best position to make the Web safer −− software vendors, Internet service providers and anti−virus software makers −− are failing to respond effectively to a snowballing threat, say security experts and industry executives.** Tech suppliers say they're doing all they can to make it easier for home users to secure their own PCs: guiding consumers to a raft of products and services they can use to lock out cyberintruders. "As long as we rely on the end user as the primary mechanism to secure their own computer, we will continue to have large quantities of unsecured devices," says Mitchell Ashley, chief technology officer at StillSecure. "They (tech suppliers) are not working together, and because they're not working together, they're putting all of us at risk," says Alan Paller, research director of SANS Institute, a Washington−based Internet−security think tank and training center. **Worldwide losses from cyberattacks will swell to an estimated $16.7 billion by the close of the year, up from $3.3 billion in 1997, according to tech consultant Computer Economics.** What's needed, security experts agree, is for tech suppliers to collaborate on implementing systemwide measures that protect consumers by default.
Source: http://www.usatoday.com/tech/news/computersecurity/2004−09−0 9−zombie−response_x.htm

27. *September 08, TechWeb.com* — **ISPs given thumbs down for virus, hacker control. U.S. residential Internet users are much more satisfied with the spam protection from their Internet service providers, but remain unhappy with their ISPs' defenses against hackers and viruses, J.D. Power and Associates said Wednesday, September 8.** In its 2004 survey of 9,500 residential customers, ISPs' ability to keep spam at bay received the largest satisfaction gains over 2003, the market researcher said. Hacker and virus protection, on the other hand, was the only one of seven factors addressed in the survey to register a decline. **The study showed that consumers are expecting ISPs to provide full Internet protection, including spam filters and protection from spyware, hackers and viruses.** The study also found that household Internet penetration in the U.S. increased by only two percent in 2004 to 66 percent. From 2002 to 2003, the percentage of U.S. households with Internet access increased by seven

percent. Despite the declining numbers, it was too soon to say Internet penetration had reached its peak. Report is available at:
http://www.jdpower.com/news/releases/pressrelease.asp?ID=200 4098
Source: http://www.techweb.com/wire/security/showArticle.jhtml?artic leID=46802751

28. *September 08, CNET News.com* — **Study: Spammers use e−mail ID to gain legitimacy. With few junk e−mail filters supporting a protocol for verifying the source address of digital messages, spammers have adopted it themselves as a way to appear more legitimate,** according to a preliminary report released on Wednesday, September 8. The author of the study, e−mail services provider MX Logic, analyzed nearly 10 million bulk e−mail messages that it had filtered on behalf of its clients in late August. **The company found that nearly a sixth of the sources of the junk messages used a protocol known as Sender Policy Framework (SPF) to certify that the e−mail addresses used in the messages were real.** While SPF has been touted as a way to stop spam, the data has shown that the true value of the protocol is more about preventing fraud, said Scott Chasin, chief technology officer of MX Logic. SPF is one of two technologies currently being considered as part of a hybrid method, dubbed Sender ID, for certifying the source of e−mail messages. Another technology, Microsoft's Caller ID for E−mail, makes up the other half of the proposed standard. The Internet Engineering Task Force, the technical committee creating the standard, debated the issues extensively over its e−mail list during the last two weeks. Report details available at:
http://www.mxlogic.com/news_events/09_08_04.html
Source: http://news.com.com/Study%3A+Spammers+use+e−mail+ID+to+gain+ legitimacy/2100−1029_3−5357269.html?tag=nefd.top

29. *September 08, TechWeb.com* — **Carriers: Build and VoIP subscribers will follow. Service providers worldwide are buying next−generation Voice over Internet Protocol (VoIP) equipment at a steady pace, as the overall number of subscribers for Internet telephony remains small, market research firm Dell'Oro Group said Wednesday, September 8.** Equipment sales, including soft switches, media gateways and hybrid gateway soft switches, increased by three percent in the second quarter to $365 million from $354 million in the first quarter. **For the full year, equipment sales are expected to rise to $1.6 billion from $1.3 billion in 2003.** Despite the market growth, the number of subscriber licenses for service providers declined quarter−to−quarter by 12 percent due to the performance of UTStarcom Inc., which accounts for more than half of all VoIP subscribers today. **Most of UTStarcom's subscribers are in China, where VoIP technology is used extensively as a substitute for traditional copper wiring found in the U.S. and Europe.** Shipments of VoIP phones used in corporations are expected to grow at an annual compounded rate of more than 20 percent in the U.S. through 2009, according to market researcher Insight Research. As a result, VoIP is expected to overtake older technology in 2009.
Source: http://www.techweb.com/wire/networking/showArticle.jhtml?art icleID=46802755

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: The US−CERT Operations Center strongly encourages Windows XP users to upgrade to Service Pack 2 if they have not already done so. SP2 offers significant protection against many of the emergent attacks that target Browser Helper Objects and Cross Domain Vulnerabilities in Internet Explorer. See http://www.us−cert.gov/cas/alerts/SA04−243A.html for more information.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 137 (netbios−ns), 1434 (ms−sql−m), 445 (microsoft−ds), 9898 (dabber), 5554 (sasser−ftp), 139 (netbios−ssn), 1026 (nterm), 3127 (mydoom), 1027 (icq) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

30. *September 09, Fresno Bee (CA)* — **Bomb threat evacuates Fresno courthouse. A bomb threat forced the evacuation of a busy Fresno County, CA, Superior Court Wednesday, September 8, bogging down a local judicial system in the middle of a four−day work week.** The bomb threat was called into the Fresno police dispatch center at 8:44 a.m. The caller told police that a bomb would be detonated at 9:30 a.m. By 9:10 a.m., acting presiding judge Edward Sarkisian Jr. had made the decision to evacuate the courthouse. Authorities twice searched the building and perimeter and found nothing suspicious. More than 1,200 cases were scheduled Wednesday in the courthouse. It is typically the busiest day of the court week. Source: http://www.fresnobee.com/local/story/9116630p−10016637c.html

31. *September 09, Associated Press* — **Mayor outlines elaborate camera network for city.** More than 2,000 surveillance cameras in public places would be tied to a network armed with software to alert authorities to suspicious behavior or emergency situations under a proposed plan announced Thursday, September 9, by Mayor Richard Daley in Chicago, IL. **The city plans to buy 250 new surveillance cameras and place them in places determined to be at high risk for crime or terrorism.** They would be networked with 30 cameras police are using to try to curb violent crime, along with more than 1,000 already at O'Hare International Airport, on the city's transit lines and in public housing buildings and schools, Daley said. The cameras wouldn't all be continuously monitored. Software would be used to pick up out−of−the ordinary activity on the incoming video images −− such as a bag being abandoned in a stairwell, a car pulling to the side of a highway, or movement in an area declared off−limits to human activity. When such suspicious behavior was noted by the software, a staff member in the city's Office

of Emergency Management would be alerted and could then notify police, medical personnel or a tow truck −− whatever the situation called for. Daley dismissed privacy concerns, saying that the only places where the city installs cameras are public spaces.
Source: http://www.chicagotribune.com/news/local/chi−040909cameras,1,5339383.story?coll=chi−news−hed

32. *September 09, Associated Press* — **Office of Montana governor, Capitol evacuated. The governor's office and a portion of the state Capitol were evacuated Thursday, September 9, after the discovery of what authorities described as a potential explosive device in a letter.** Barbara Ranf, chief of staff for Governor Judy Martz, said a staff member was opening a letter that apparently contained a match, which ignited and began burning paper. The letter also contained a fuse and small plastic bag, but Ranf said it appeared the fuse did not ignite. There was no explosion and no one was injured. It was not immediately clear what, if anything, was in the plastic bag. The governor was not in the Capitol at the time, Ranf said. Sheryl Olson, deputy administrator of the General Services Division, said the evacuation of the second and third floors of the Capitol's east wing was ordered because police considered the incident a "credible threat."
Source: http://abcnews.go.com/wire/US/ap20040909_1166.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer